What is claimed is:

1.   A method for providing communications system security, comprising:

establishing communications between a first communications device and a communications server;

generating a token in said communications server;

5   providing said token to said first communications device;

entering identifying information in said first communications device;

establishing communications between said first communications device and a security server;

providing said identifying information and said token to said security server;

10   encrypting said token in said security server;

providing said encrypted token to said first communications device;

providing said encrypted token to said communications server;

receiving said encrypted token at said communications server; and

granting said first communications device access to said communications system.

2.   The method of Claim 1, wherein said security server utilizes said identifying information as an encryption key.

3.   The method of Claim 1, wherein said identifying information comprises at least one of a user identifier and a user password.

4.   The method of Claim 1, wherein said step of establishing communications

comprises requesting that a communications extension assigned to a second

communications device be transferred to said first communications device.

5.   The method of Claim 4, wherein said step of granting said first

communications device access to said communications system comprises granting said

request to transfer said communications extension to said first communications device,

wherein at least a first plurality of communications features available to a user through

said second communications device when said second communications device is assigned

to said extension are available to a user through said first communications device when

said first communications device is assigned to said extension.

6.   The method of Claim 1, wherein said communications system comprises a

private branch exchange telephony system.

7.   The method of Claim 1, further comprising:

altering an encryption algorithm in said security server;

altering a decryption algorithm in said communications server to correspond to

said altered encryption algorithm in said security server, wherein a token passed to said

security server by said first communications device and encrypted by said security server

using said altered encryption algorithm and said identifying information can be decrypted

by said communications server using said altered decryption algorithm.

8.   The method of Claim 1, wherein said first communications device comprises a personal digital assistant.

9.   The method of Claim 1, wherein said first communications device establishes communications with said communications server over a communications network comprising at least one of a wireless network, a wired network, and a switched voice data network.

10.   The method of Claim 1, wherein said step of providing said encrypted token to said communication server is performed after said encrypted token is received at said first communications device.

11.   The method of Claim 1, wherein said step of granting said first communications device access to said communication system comprises:

applying said encrypted token received at said communication server; and

verifying that said decrypted token matches said encrypted token generated in said

5   communications server.

12.   The method of Claim 1, wherein an encryption algorithm used in connection with determining whether to grant access to said communications system is not stored in said first communications device.

-16-

13. A communications system providing remote security, comprising:

a) a communications network;

b) a system server, comprising:

    i)   communication system software;

    ii)   decryption software; and

    iii)   a network interface interconnected to said communications

network;

c) a first communications device, comprising:

    i) communications device software;

    ii) a network interface interconnected to said communications network;

d) a security server, comprising:

    i) encryption software; and

    ii) a network interface interconnected to said communications network,

wherein said first communications device is in communication with said security

server and with said system server, and wherein said first communications device

is granted access to said system server in response to receipt by said system server

of a token encrypted by said security server.

14. The communications system of Claim 13, wherein said communications

network comprises at least one of a wireless computer network, a wired computer

network, and a switched voice data network.

15. The communications system of Claim 13, wherein said first

-17-

communications device comprises at least one of a soft telephone and a hard telephone.

16. The communications system of Claim 13, wherein said first communications device comprises a personal digital assistant.

17. The communications system of Claim 13, wherein said first communications device is capable of providing a first set of functions provided by a second communications device comprising a hard telephone when said first communications device is granted access to said system server.

18. The communications system of Claim 13, wherein an encryption algorithm for use in connection with said communications system is not stored on said communications device.

19.   A communications system with security features remote from a communication device, comprising:

at least a first communications device;

means for encrypting information received from said at least a first

5   communications device, wherein said means for encrypting are located remotely from said at least a first communications device;

means for providing communications services to a plurality of communications devices, including said at least a first communications device and at least a second communications device; and

10   means for interconnecting said at least a first communications device to said means for encrypting information and to said means for providing communications services, wherein said at least a first communications device is operable to perform at least a first set of communications functions.

20.   The communications system of Claim 19, further comprising:

means for interconnecting said at least a second communications device to said means for providing communications services, wherein said at least a second communications device is operable to perform said at least a first set of communications

5   functions, and wherein an extension assigned to said at least a second communications device is reassigned to said at least a first communications device.

21.   The communication system of Claim 19, wherein said means for

interconnecting said at least a first communications device to said means for encrypting

information and to said means for providing communications services comprises a

wireless communications channel.